Action
CCA 86-2034

Legislation

OFFICE OF CONGRESSIONAL AFFAIRS
Routing Slip

	ACTION	INFO
1. D/OCA		X
2. DD/Legislation		
3. DD/Senate Affairs		X
4. Ch/Senate Affairs		
5. DD/House Affairs		X
6. Ch/House Affairs		
7. Admin Officer		
8. Executive Officer		X
9. FOIA Officer		
10. Constituent Inquiries Officer		
11.		
12.		

SUSPENSE   20 June 86

Date

Action Officer

Remarks: Action completed 6/18/86

~~Defer to NSA~~ Told OMB that we share NSA concerns and oppose 6.7/ GJ / 16 June 86

Name/Date

File - Computers.

STAT

STAT

Action
XA 86-2034

OFFICE OF CONGRESSIONAL AFFAIRS
Routing Slip

	ACTION	INFO
1. D/OCA		x
2. DD/Legislati		
3. DD/Senate A......		x
4. Ch/Senate Affairs		
5. DD/House Affairs		x
6. Ch/House Affairs		
7. Admin Officer		
8. Executive Officer		x
9. FOIA Officer		
10. Constituent Inquiries Officer		
11.		
12.		

SUSPENSE   20 June 86
Date

Action Officer:

Remarks:

CJ / 16 June 86
Name/Date

STAT

STAT

OCA FILE _Legislation_ | CONGRESSIONAL AFFAIRS

RECPT # _Chrono_ | 86 - 2034

SPECIAL

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

SPECIAL

June 12, 1986

LEGISLATIVE REFERRAL MEMORANDUM

TO:

Department of Commerce - Joyce Smith (377-4264)
Department of Defense - Werner Windus (697-1398)
Department of State - Lee Ann Berkenbile (647-4463)
Department of the Treasury - Carole Toth (566-8523)
Department of Justice - Jack Perkins (633-2113)
General Services Administration
National Security Council
Central Intelligence Agency
Office of Personnel Management - Jim Woodruff (632-4682)
Department of Energy - Bob Rabben (252-6718)

SUBJECT: H.R. 2889 -- Computer Security Act -- as ordered
reported by the House Science and Technology Committee
on June 4, 1986. (A copy of the amended version is
attached.)

The Office of Management and Budget requests the views of your
agency on the above subject before advising on its relationship to
the program of the President, in accordance with Circular A-19.

Please provide us with your views no later than June 20, 1986.

Direct your questions to Connie Bowers (395-3457), of this office.

James C. Murr for
Assistant Director for
Legislative Reference

Enclosures
cc: Ed Springer
      Arnold Donahue
      Kevin Scheid
      Sheri Alpert

H2889K

As ordered reported by H. Sci. & Tech.
6/4/86

[COMMITTEE PRINT]

June 3, 1986

SUBSTITUTE AMENDMENT OFFERED BY MR. GLICKMAN
FOR THE SUBCOMMITTEE AMENDMENT TO H.R. 2889

Strike out all after the enacting clause and insert in lieu thereof the following:

1 **SECTION 1. SHORT TITLE.**

2   This Act may be cited as the ``Computer Security Act of

3 1986´´.

4 **SEC. 2. PURPOSE.**

5   (a) IN GENERAL.--The Congress declares that improving the

6 security and privacy of sensitive information in Federal

7 computer systems is in the public interest, and hereby

8 creates a means for establishing minimum acceptable security

9 practices for such systems, without limiting the scope of

10 security measures already planned or in use.

11   (b) SPECIFIC PURPOSES.--The purposes of this Act are--

12   (1) to assign to the National Bureau of Standards

13   responsibility for developing standards and guidelines

14   for Federal computer systems, including standards and

15   guidelines needed to assure the cost-effective security

1   and privacy of sensitive information in Federal computer

2   systems, by amending the Act of March 3, 1901;

3   (2) to provide for promulgation of such standards and

4   guidelines by amending section 111(f) of the Federal

5   Property and Administrative Services Act of 1949;

6   (3) to require establishment of security plans by all

7   operators of Federal computer systems that contain

8   sensitive information; and

9   (4) to require mandatory periodic training for all

10   persons involved in management, use, or operation of

11   Federal computer systems that contain sensitive

12   information.

13   **SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.**

14   The Act of March 3, 1901 (15 U.S.C. 271-278h), is

15   amended--

16   (1) in section 2(f), by striking out ``and´´ at the

17   end of paragraph (18), by striking out the period at the

18   end of paragraph (19), and by inserting after such

19   paragraph the following:

20   ``(20) the study of equipment, procedures, and

21   systems for automatic acquisition, storage, manipulation,

22   display, and transmission of information, and its use to

23   control machinery and processes.´´;

24   (2) by redesignating section 18 as section 20, and by

25   inserting after section 17 the following new sections:

3

1   ``SEC. 18. (a) The National Bureau of Standards shall--

2   ``(1) have the mission of developing standards,

3   guidelines, and associated methods and techniques for

4   computer systems;

5   ``(2) except as described in paragraph (3) of this

6   subsection (relating to security standards), develop

7   uniform standards and guidelines for Federal computer

8   systems, except those systems excluded by section 2315 of

9   title 10, United States Code, or section 3502(2) of title

10   44, United States Code;

11   ``(3) have responsibility within the Federal

12   Government for developing technical, management, and

13   administrative standards and guidelines for the cost-

14   effective security and privacy of sensitive information

15   in Federal computer systems except--

16   ``(A) those systems excluded by section 2315 of

17   title 10, United States Code, or section 3502(2) of

18   title 44, United States Code; and

19   ``(B) those systems which are protected at all

20   times by procedures established for information which

21   has been specifically authorized under criteria

22   established by an Executive order or an Act of

23   Congress to be kept secret in the interest of

24   national defense or foreign policy,

25   the primary purpose of which standards and guidelines

4

1   shall be to control loss and unauthorized modification or

2   disclosure of sensitive information in such systems and

3   to prevent computer-related fraud and misuse;

4   ``(4) submit standards and guidelines developed

5   pursuant to paragraphs (2) and (3) of this subsection,

6   along with recommendations as to the extent to which

7   these should be made compulsory and binding, to the

8   Secretary of Commerce, for promulgation under section 111

9   of the Federal Property and Administrative Services Act

10   of 1949;

11   ``(5) develop guidelines for use by operators of

12   Federal computer systems that contain sensitive

13   information in training their employees in security

14   awareness and accepted security practice, as required by

15   section 5 of the Computer Security Act of 1986; and

16   ``(6) develop validation procedures for, and evaluate

17   the effectiveness of, standards and guidelines developed

18   pursuant to paragraphs (1), (2), and (3) of this

19   subsection through research and liaison with other

20   government and private agencies.

21   ``(b) In fulfilling subsection (a) of this section, the

22   National Bureau of Standards is authorized--

23   ``(1) to assist the private sector in using and

24   applying the results of the programs and activities under

25   this section;

5

1   ``(2) to make recommendations, as appropriate, to the

2   Administrator of General Services on policies and

3   regulations proposed pursuant to section 111(f) of the

4   Federal Property and Administrative Services Act of 1949;

5   ``(3) as requested, to provide to operators of

6   Federal computer systems technical assistance in

7   implementing the standards and guidelines promulgated

8   pursuant to section 111(f) of the Federal Property and

9   Administrative Services Act of 1949;

10   ``(4) to assist, as appropriate, the Office of

11   Personnel Management in developing regulations pertaining

12   to training, as required by section 5 of the Computer

13   Security Act of 1986;

14   ``(5) to perform research and to conduct studies, as

15   needed, to determine the nature and extent of the

16   vulnerabilities of, and to devise techniques for the cost

17   effective security and privacy of sensitive information

18   in Federal computer systems; and

19   ``(6) to coordinate closely with other agencies and

20   offices (including, but not limited to, the Departments

21   of Defense and Energy, the National Security Agency, the

22   General Accounting Office, the Office of Technology

23   Assessment, and the Office of Management and Budget)--

24   ``(A) to assure maximum use of all existing and

25   planned programs, materials, studies, and reports

6

1   relating to computer systems security and privacy, in

2   order to avoid unnecessary and costly duplication of

3   effort; and

4   ``(B) to assure, to the maximum extent feasible,

5   that standards developed pursuant to subsection

6   (a)(3) and (5) are consistent and compatible with

7   standards and procedures developed for the protection

8   of information in Federal computer systems which is

9   authorized under criteria established by Executive

10   order or an Act of Congress to be kept secret in the

11   interest of national defense or foreign policy.

12   ``(c) As used in this section and section 19, the terms

13 `computer system´, `Federal computer system´, `operator of a

14 Federal computer system´, and `sensitive information´ have

15 the meanings given in section 7 of the Computer Security Act

16 of 1986.

17   ``SEC. 19. (a) There is hereby established a Computer

18 System Security and Privacy Advisory Board within the

19 Department of Commerce. The Secretary of Commerce shall

20 appoint the chairman of the Board. The Board shall be

21 composed of twelve additional members appointed by the

22 Secretary of Commerce as follows:

23   ``(1) four members from outside the Federal

24   Government who are eminent in the computer or

25   telecommunications industry, at least one of whom is

H2889K

7

1   representative of small or medium sized companies in such

2   industry;

3   `` (2) four members from outside the Federal

4   Government who are eminent in the fields of computer or

5   telecommunications technology, or related disciplines,

6   but who are not employed by or representative of a

7   producer of computer or telecommunications equipment; and

8   `` (3) four members from the Federal Government who

9   have computer systems management experience, including

10   experience in computer systems security and privacy, at

11   least one of whom shall be from the National Security

12   Agency.

13   `` (b) The duties of the Board shall be--

14   `` (1) to identify emerging managerial, technical,

15   administrative, and physical safeguard issues relative to

16   computer systems security and privacy;

17   `` (2) to advise the Bureau of Standards and the

18   Secretary of Commerce on security and privacy issues

19   pertaining to Federal computer systems; and

20   `` (3) to report its findings to the Secretary of

21   Commerce, the Director of the Office of Management and

22   Budget, the Director of the National Security Agency, and

23   the appropriate Committees of the Congress.

24   `` (c) The term of office of each member of the Board

25   shall be four years, except that--

1   ``(1) of the initial members, three shall be

2   appointed for terms of one year, three shall be appointed

3   for terms of two years, three shall be appointed for

4   terms of three years, and three shall be appointed for

5   terms of four years; and

6   ``(2) any member appointed to fill a vacancy in the

7   Board shall serve for the remainder of the term for which

8   his predecessor was appointed.

9   ``(d) The Board shall not act in the absence of a quorum,

10   which shall consist of seven members.

11   ``(e) Members of the Board, other than full-time

12   employees of the Federal Government, while attending meetings

13   of such committees or while otherwise performing duties at

14   the request of the Board Chairman while away from their homes

15   or a regular place of business, may be allowed travel

16   expenses in accordance with subchapter I of chapter 57 of

17   title 5, United States Code.

18   ``(f) To provide the staff services necessary to assist

19   the Board in carrying out its functions, the Board may

20   utilize personnel from the National Bureau of Standards or

21   any other agency of the Federal Government with the consent

22   of the head of the agency.´´; and

23   (3) by adding at the end thereof the following new

24   section:

25   ``SEC. 21. This Act may be cited as the National Bureau

H2889K

9

1 of Standards Act.``.

2 **SEC. 4. AMENDMENT TO BROOKS ACT.**

3   Section 111(f) of the Federal Property and Administrative

4 Services Act of 1949 (40 U.S.C. 759(f)) is amended to read as

5 follows:

6   ``(f)(1) The Secretary of Commerce shall, on the basis of

7 standards and guidelines developed by the National Bureau of

8 Standards pursuant to section 18(a)(2) and (3) of the

9 National Bureau of Standards Act, promulgate standards and

10 guidelines pertaining to Federal computer systems, making

11 such standards compulsory and binding to the extent to which

12 the Secretary determines necessary to improve the efficiency

13 of operation or security and privacy of Federal computer

14 systems.

15   ``(2) The head of a Federal agency may employ standards

16 for the cost effective security and privacy of sensitive

17 information in a Federal computer system within or under the

18 supervision of that agency that are more stringent than the

19 standards promulgated by the Secretary of Commerce, if such

20 standards contain, at a minimum, the provisions of those

21 applicable standards made compulsory and binding by the

22 Secretary of Commerce.

23   ``(3) The standards determined to be compulsory and

24 binding may be waived by the Secretary of Commerce in writing

25 upon a determination that compliance would adversely affect

1 the accomplishment of the mission of an operator of a Federal

2 computer system, or cause a major adverse financial impact on

3 the operator which is not offset by government-wide savings.

4 The Secretary may delegate to the head of one or more Federal

5 agencies authority to waive such standards to the extent to

6 which the Secretary determines such action to be necessary

7 and desirable to allow for timely and effective

8 implementation of Federal computer systems standards. The

9 head of such agency may redelegate such authority only to a

10 senior official designated pursuant to section 3506(b) of

11 title 44, United States Code. Notice of each such waiver and

12 delegation shall be promptly transmitted to the Committee on

13 Government Operations of the House of Representatives and the

14 Committee on Governmental Affairs of the Senate.

15 ``(4) The Administrator shall ensure that such standards

16 and guidelines are implemented within an integrated

17 information resources management system (as required by

18 chapter 35 of title 44, United States Code) by--

19 ``(A) developing and implementing policies on Federal

20 computer systems; and

21 ``(B) revising the Federal information resources

22 management regulations (41 CFR ch. 201) to implement such

23 standards, guidelines, and policies.

24 ``(5) As used in this section, the terms `computer

25 system`, operator of a Federal computer system`, and `Federal

H2889K

11

1 computer system' have the meanings given in section 7 of the

2 Computer Security Act of 1986.''.

3 SEC. 5. TRAINING BY OPERATORS OF FEDERAL COMPUTER SYSTEMS.

4   (a) IN GENERAL.--Each operator of a Federal computer

5 system that contains sensitive information shall provide

6 mandatory periodic training in computer security awareness

7 and accepted computer security practice. Such training shall

8 be provided under the guidelines developed pursuant to

9 section 18(a)(5) of the the National Bureau of Standards Act

10 (as added by section 3 of this Act), and in accordance with

11 the regulations issued under subsection (c) of this section,

12 for all employees who are involved with the management, use,

13 or operation of computer systems.

14   (b) TRAINING OBJECTIVES.--Training under this section

15 shall be started within 60 days after the issuance of the

16 regulations described in subsection (c). Such training shall

17 be designed--

18   (1) to enhance employees' awareness of the threats to

19   and vulnerability of computer systems; and

20   (2) to encourage the use of improved computer

21   security practices.

22   (c) REGULATIONS.--Within six months after the date of the

23 enactment of this Act, the Director of the Office of

24 Personnel Management shall issue regulations prescribing the

25 procedures and scope of the training to be provided under

1 subsection (a) and the manner in which such training is to be

2 carried out.

3 SEC. 6. ADDITIONAL RESPONSIBILITIES FOR OPERATORS OF FEDERAL

4   COMPUTER SYSTEM FOR COMPUTER SYSTEMS SECURITY

5   AND PRIVACY.

6   (a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE

7 INFORMATION.--Within 6 months after the date of enactment of

8 this Act, each operator of a Federal computer system shall

9 identify each computer system, and system under development,

10 of that operator which contains sensitive information.

11   (b) SECURITY PLAN.--Within one year after the date of

12 enactment of this Act, each such operator shall, consistent

13 with the standards, guidelines, policies, and regulations

14 prescribed pursuant to section 111(f) of the Federal Property

15 and Administrative Services Act of 1949, establish a plan for

16 the security and privacy of the computer systems identified

17 pursuant to subsection (a). Copies of such plan shall be

18 transmitted to the National Bureau of Standards and the

19 National Security Agency for advice and comment. In the case

20 of a Federal contractor or other organization, such plan

21 shall be transmitted through its supervising Federal agency.

22 Such plan shall be subject to disapproval by the Director of

23 the Office of Management and Budget.

24 SEC. 7. DEFINITIONS.

25   As used in this Act, sections 18 and 19 of the National

H2889K

13

1   Bureau of Standards Act, and section 111(f) of the Federal

2   Property and Administrative Services Act of 1949--

3   (1) the term ``computer system´´ means an

4   interconnected collection of equipment and procedures for

5   the automatic acquisition, storage, manipulation,

6   display, and any associated equipment and procedures for

7   electromagnetic transmission of information to or from

8   such collection;

9   (2) the term ``Federal computer system´´ means a

10   computer system operated by a Federal agency (as that

11   term is defined in section 3(b) of the Federal Property

12   and Administrative Services Act of 1949) or by a

13   contractor of a Federal agency or other organization that

14   processes information for the Federal Government using a

15   computer system;

16   (3) the term ``operator of a Federal computer

17   system´´ means a Federal agency (as that term is defined

18   in section 3(b) of the Federal Property and

19   Administrative Services Act of 1949), contractor of a

20   Federal agency, or other organization that processes

21   information for the Federal Government using a computer

22   system; and

23   (4) the term ``sensitive information´´ means any

24   information, the loss, misuse, or unauthorized

25   modification of which could adversely affect the national

14

1   interest or the conduct of Federal programs, or the

2   privacy to which individuals are entitled under section

3   552 of title 5, United States Code (the Privacy Act), but

4   which has not been specifically authorized under criteria

5   established by an Executive order or an Act of Congress

6   to be kept secret in the interest of national defense or

7   foreign policy.

8 **SEC. 8. AUTHORIZATION OF APPROPRIATIONS.**

9   There are authorized to be appropriated to each Federal ·

10 agency such sums as may be necessary for fiscal years 1987,

11 1988, and 1989 to carry out the computer systems security

12 training program established by section 5 of this Act and the

13 identification and planning requirements of section 6.

Amend the title so as to read: ``A bill to amend the Act
establishing the National Bureau of Standards to provide for
a computer standards program within such Bureau, to provide
for government-wide computer security, and to provide for the
training in security matters of persons who are involved in
the management, operation, and use of Federal computer
systems.''.